UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,625	05/08/2001	Rajasekhar Sistla	P10212	3678

50890 7590 03/02/2011

Caven & Aghevli LLC
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
TRUONG, LAN DAI T	

ART UNIT	PAPER NUMBER
2452	

MAIL DATE	DELIVERY MODE
03/02/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/851,625	**Applicant(s)** SISTLA, RAJASEKHAR	
	Examiner LAN-DAI Thi TRUONG	**Art Unit** 2452	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 May 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is response to Request for Continued Examination (RCE) filed on 12/01/2010. Claims 1-21 are pending; claims 1, 6, 11 and 17 are amended.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/01/2010 has been entered.

3. The applicant's arguments filed on 12/01/2010 have fully considered but they are moot in view with new ground for rejections.

Claim Objections

4. Claim 7 is objected to because of the following informalities: the claim recites element "the email client" which lacks antecedent basis. In view of examiner, this element should be either the recipient email client/ or the sender email client. Appropriate correction is required. For examination purpose, examiner will interpret 'the mail client' as the recipient email client.

Examiner interpretations

5. Claim 1 is directed to statutory subject matter under meaning of 35 U.S.C § 101 because of claim features 'encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage; and decrypting the electronic mail, at the recipient if the recipient attempts to retrieve the electronic mail from the local storage'. Those steps could not be performed either mentally, verbally or

without a machine. Those steps inherently invoke/require a machine or article for implementations.

6. Claim 17 is directed to statutory subject matter under meaning of 35 U.S.C § 101 of follow reasons: the specification is silent in regarding a definition or evidence in that a device includes signals, therefore claim element 'storage device' should be interpreted with it's ordinary meaning which would be only machines and not a signal.

Claim rejections-35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 6-16 are rejected under 35 U.S.C 101 as directed to non-statutory subject matter.

Regarding claims 6-10:

Claim 6 is directed to non-statutory subject matter because of follow reasons:

The claim is directed to statutory subject matter only if at least one of the claimed elements is a physical part of a device.

The specification is silent in regarding actual definitions for claims elements (an electronic mail confidentiality preserver, input-processing engine; encryption/description engine) as directed to a physical components; therefore, applying the broadest reasonable interpretation, 'engine' could be equally implemented as software component (e.g. as a portion of program) (see, 'Microsoft Computer Dictionary, fifth edition, page 193), and preserver could be equally implemented as software (see 'Microsoft Computer Dictionary, fifth edition, page 474);

therefore claim 6 lacks the necessary structure element; thus, claim 6 and its dependencies fail to fall within one of the four statutory categories of invention recited in 35 U.S.C. § 101 process, machine, manufacture, and composition of matter, and directed to non-statutory subject matter.

Regarding claims 11-16:

Claim 11 is directed to non-statutory subject matter because of follow reasons:

The claim is directed to statutory subject matter only if at least one of the claimed elements is a physical part of a device.

The specification is silent in regarding actual deifications for claims elements (local storage; communication engine, an electronic mail confidentiality preserver, input-processing engine; encryption; description engine) as directed to a physical components; therefore, applying the broadest reasonable interpretation, 'local storage' could be equally implemented as a data file (see 'American Heritage College dictionary, page 1362), 'engine' could be equally implemented as software component (e.g. as a portion of program) (see, 'Microsoft Computer Dictionary, fifth edition, page 193), and preserver could be equally implemented as software (see 'Microsoft Computer Dictionary, fifth edition, page 474).

Furthermore, It would have been obvious to one of ordinary skill in the art to understand that claim element 'user interface' is directed to a software component, see ('Microsoft Computer Dictionary, fifth edition, page 544).

Therefore, claim 11 lacks the necessary structure element; thus, claim 11 and its dependencies fail to fall within one of the four statutory categories of invention recited in 35 U.S.C. § 101 process, machine, manufacture, and composition of matter, and directed to non-statutory subject matter.

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C 103(a) as being un-patentable Ross (U.S. 2002/0143885) in view of Spraggs (U.S. 6,941,454) further in view of Kobata et al. (U.S. 2003/0023695)

<u>Regarding claim 1:</u>

Ross discloses the invention substantially as claimed, including a method for preserving confidentiality of an electronic mail from a sender to a recipient, comprising:

the sender and the recipient are each directly coupled to communicate with both the authentication server and the mail server: (both email sender and email receiver are each directly coupled to mail server and authentication server module: Ross, figure 1, items 118, 136; [0080]).

authenticating identity information of the recipient based on data provided by an authentication server: (authenticating email user passwords/ company badge: Ross, [0061]).

decrypting the electronic mail, at the recipient: (recipient decrypts received encrypted email message: Ross, [0142]; [0183]).

However, Ross does not explicitly disclose encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail, at the recipient if the recipient attempts to retrieve the electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made combine Spraggs'ideas of decrypting the stored re-encrypted data when attempting to retrieve the data from the secure database and re-encrypting data for storing into a secure database into Ross' system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

However, Ross-Spraggs does not explicitly disclose restricting the recipient's ability to modify contents of the electronic mail, from a mail server, based on a confidentiality level established by the sender, wherein a user interface is to comprise a first set of confidentiality levels from which the sender is to select.

In analogous art, Kobata discloses a mail client with capabilities setting secure email delivery options, such as, through a user interface with a set of selectable functions (i.e. "send secure;" "preventing forwarding;" "preventing copy" …etc.), the sender could set restrictions options for recipient's ability to modify receiving content, see (Kobata, [0212]; [0219]; [0220]; [0227]; [0159]-[0160]; [0029]; figures 26 & 28 & 37 & 38; [0215]).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kobata's ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Ross-Spraggs's system in order to provide an efficient and secure email delivery system (see Kobata, [0008]-[0009]).

Regarding claim 2:

In addition to rejection in claim 1, Ross-Kobata-Spraggs further discloses wherein the identity information is a system password: (providing user IDs and Passwords for authentication process: Kobata, [0070]).

Regarding claim 3:

In addition to rejection in claim 1, Ross-Spraggs-Kobata further discloses prompting a user of the recipient to supply the identity information: (a receiver is requested to provide user IDs and Passwords for authentication process: Kobata, [0070]).

decrypting the electronic mail with the identity information supplied by the user: (in Spraggs's system, the receiving client can decrypt data via using it's private key: column 3, lines 65-67).

Regarding claim 4:

In addition to rejection in claim 1, Ross-Spraggs-Kobata further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (by using Atabok Digital Asset control option, sender can select/update modification options. It would have been obvious to one of ordinary skill in the art to understand that when new option is selected, the original selected would be disabled: Kobata, [0220]; [0212]; figure 28).

Regarding claim 5:

In addition to rejection in claim 4, Ross-Spraggs-Kobata further discloses the control signal is a control signal: (message senders and message receivers can operate in a non-graphical environment by entering command line operations according to compatible protocols: Kobata, [0062]).

Regarding claim 6:

Ross discloses the invention substantially as claimed, including an electronic mail confidentiality preserver of a recipient email client, which can be implemented in a computer hardware or software code, comprising:

the sender and the recipient are each directly coupled to communicate with both the authentication server and the mail server: (both email sender and email receiver are each directly coupled to mail server and authentication server module: Ross, figure 1A, items 118, 136; [0080]).

However, Ross does not explicitly disclose an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information based on data provided by an authentication server if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses communications between a sever and a client. The server, including encryption/decryption engine coupled to input engine. The server encrypts an email by using user private keys (Spraggs, figure 8, items 802, 804, 806, 812, 814; figure 2, item

200; figure 3, items 306). The server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "server" of Spraggs with capabilities of decrypting the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests and re-encrypting data prior storing them into a secure database to 'recipient' as taught in Ross. The combination would have been obvious because one of ordinary skill in the art would have been motivated to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

However, Ross-Spraggs does not explicitly disclose limit abilities of a user of the recipient email client to modify contents of an electronic mail received by the recipient email client based on a confidentiality level, wherein a user interface further comprises a first set of confidentiality levels from which a user of a sender email client is to select.

In analogous art, Kobata discloses a mail client with capabilities setting secure email delivery options, such as, through a graphical user interface with a set of selectable functions (i.e. "send secure;" "preventing forwarding;" "preventing copy" …etc.), the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0212]; [0219]; [0220]; [0227]; [0159]-[0160]; [0029]; figures 26 & 28 & 37 & 38; [0215]).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kobata's ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Ross-Spraggs's system in order to provide an efficient and secure email delivery system (see, [0008]-[0009]).

Regarding claim 7:

In addition to rejection in claim 6, Ross-Spraggs-Kobata further discloses asserts a first control signal to disable options that are originally supported by the email client if the confidentiality level satisfies a predefined confidentiality threshold: (by using Atabok Digital Asset control option, sender can select/update modification options. It would have been obvious to one of ordinary skill in the art to understand that when new option is selected, the original selected would be disabled: Kobata, [0220]; [0212]; figure 28).

Regarding claim 8:

In addition to rejection in claim 7, Ross-Spraggs-Kobata further discloses the control signal is a control signal: (message senders and message receivers can operate in a non-graphical environment by entering command line operations according to compatible protocols: Kobata, [0062]).

Regarding claim 9:

In addition to rejection in claim 6, Ross-Spraggs-Kobata further discloses asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (recipient decrypts received encrypted email message: Ross, [0142]; [0183]).

Regarding claim 10:

In addition to rejection in claim 6, Ross-Spraggs-Kobata further discloses prompting the user for identity information: (prompting for user passwords: Spraggs: figure 6, item 606; figure 7, items 710).

decrypting the electronic email with an identity information: (decrypting email using client's receiving private key: Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database: Spraggs, column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database: Spraggs, column 3, lines 45-67).

Regarding claim 11:

Ross discloses the invention substantially as claimed, including a electronic mail clients, comprising:

the sender and the recipient are each directly coupled to communicate with both the authentication server and the mail server: (both email sender and email receiver are each directly coupled to mail server and authentication server module: Ross, figure 1A, items 118, 136; [0080]).

a user interface: (Ross: figures 5; figure 7).

a communication engine: (network interface card included in client computers: Ross, figure 3).

a local storage: (email storage: Ross, figure 318).

an electronic mail confidentiality preserver (email server: Ross, figure 1, item 118), coupled to the user interface (communication connection between client computer and email server; wherein the client computer comprises user interface: Ross: figure 1A; figures 5; figure 7), coupled to the communication engine (authentication module: Ross, figure 1A, item 136) and coupled to the local storage (email storage: Ross, figure 1A, item 140).

However, Ross does not explicitly disclose the electronic mail confidentiality preserver further comprises: an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information based on data provided by an authentication server if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses communications between a sever and a client. The server, including encryption/decryption engine coupled to input engine. The server encrypts an email by using user private keys (Spraggs, figure 8, items 802, 804, 806, 812, 814; figure 2, item 200; figure 3, items 306). The server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify “server” of Spraggs with capabilities of decrypting the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests and re-encrypting data prior storing them into a secure database to ‘recipient’ as taught in Ross. The combination would have been obvious because one of ordinary skill in the art would have been motivated to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

However, Ross-Spraggs does not explicitly disclose limit abilities of a user of the recipient email client to modify contents of an electronic mail received at the recipient email client from a sender through a email server based on a user-selected confidentiality level; wherein the user interface further comprises a first set of confidentiality levels from which a user is to select.

In analogous art, Kobata discloses a mail client with capabilities setting secure email delivery options, such as, through a graphical user interface with a set of selectable functions (i.e. “send secure;” “preventing forwarding;” “preventing copy” …etc.), the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0212]; [0219]; [0220]; [0227]; [0159]-[0160]; [0029]; figures 26 & 28 & 37 & 38; [0215]).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kobata’s ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Ross-Spraggs’s system in order to provide an efficient and secure email delivery system (see, [0008]-[0009]).

Regarding claim 12:

In addition to rejection in claim 11, Ross-Spraggs-Kobata further discloses wherein the user interface further comprises a second set of options to manipulate the electronic mail from which the user is to select: (a user interface comprise a set of selectable functions (i.e. “send secure;” “preventing forwarding;” “preventing copy”; “receiving address"....etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; [0221]; figures 26; figure 28; figure 29; figure 30; [0215]).

Regarding claim 13:

In addition to rejection in claim 12, Ross-Spraggs-Kobata further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (by using Atabok Digital Asset control option, sender can select/update modification options. It would have been obvious to one of ordinary skill in the art to understand that when new option is selected, the original selected would be disabled: Kobata, [0220]; [0212]; figure 28).

Regarding claim 14:

In addition to rejection in claim 13, Ross-Spraggs-Kobata further discloses the control signal is a control signal: (message senders and message receivers can operate in a non-graphical environment by entering command line operations according to compatible protocols: Kobata, [0062]).

Regarding claim 15:

In addition to rejection in claim 12, Ross-Spraggs-Kobata further discloses asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (recipient decrypts received encrypted email message: Ross, [0142]; [0183]).

Regarding claim 16:

In addition to rejection in claim 12, Ross-Spraggs-Kobata further discloses prompting the user for identity information: (Spraggs: figure 7, items 710, 712).

decrypting the electronic email with the identity information: (decrypting email using client's receiving private key: Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database: Spraggs, column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database: Spraggs, column 3, lines 45-67).

Regarding claim 17:

Ross discloses the invention substantially as claimed, including a storage device including a plurality of instructions readable therefrom, the instructions, when executed by a computer system, cause the computer system to perform operations comprising:

the sender and the recipient are each directly coupled to communicate with both the authentication server and the mail server: (both email sender and email receiver are each directly coupled to mail server and authentication server module: Ross, figure 1, items 118, 136; [0080]).

authenticating identity information of the recipient based on data provided by an authentication server: (authenticating email user passwords/ company badge: Ross, [0061]).

decrypting the electronic mail, at the recipient: (recipient decrypts received encrypted email message: Ross, [0142]; [0183]).

However, Ross does not explicitly disclose encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail, at the recipient if the recipient attempts to retrieve the electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made combine Spraggs'ideas of decrypting the stored re-encrypted data when attempting to retrieve the data from the secure database and re-encrypting data for storing into a secure database into Ross' system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

However, Ross-Spraggs does not explicitly disclose restricting the recipient's ability to modify contents of the electronic mail, from a mail server, based on a confidentiality level established by the sender of electronic email, wherein a user interface is to comprise a first set of confidentiality levels from which the sender is to select.

In analogous art, Kobata discloses a mail client with capabilities setting secure email delivery options, such as, through a user interface with a set of selectable functions (i.e. "send secure;" "preventing forwarding;" "preventing copy" …etc.), the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0212]; [0219]; [0220]; [0227]; [0159]-[0160]; [0029]; figures 26 & 28 & 37 & 38; [0215]).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kobata's ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Ross-Spraggs's system in order to provide an efficient and secure email delivery system (see Kobata, [0008]-[0009]).

Regarding claim 18:

In addition to rejection in claim 17, Ross-Kobata-Spraggs further discloses wherein the identity information is a system password: (providing user IDs and Passwords for authentication process: Kobata, [0070]).

Regarding claim 19:

In addition to rejection in claim 17, Ross-Spraggs-Kobata further discloses prompting a user of the recipient to supply the identity information: (a receiver is requested to provide user IDs and Passwords for authentication process: Kobata, [0070]).

decrypting the electronic mail with the identity information supplied by the user: (In Spraggs's system, the receiving client can decrypt data via using it's private key: column 3, lines 65-67).

Regarding claim 20:

In addition to rejection in claim 17, Ross-Spraggs-Kobata further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (by using Atabok Digital

Asset control option, sender can select/update modification options. It would have been obvious to one of ordinary skill in the art to understand that when new option is selected, the original selected would be disabled: Kobata, [0220]; [0212]; figure 28).

Regarding claim 21:

In addition to rejection in claim 20, Ross-Spraggs-Kobata further discloses the control signal is a control signal: (message senders and message receivers can operate in a non-graphical environment by entering command line operations according to compatible protocols: Kobata, [0062]).

Conclusions

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAN-DAI Thi TRUONG whose telephone number is (571)272-7959. The examiner can normally be reached on Monday- Friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thu Nguyen can be reached on 571-272-6967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

02/22/2011
/Lan-Dai Thi Truong/
Examiner, Art Unit 2452